Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 78 (2016) 330 – 335

Procedia Computer Science

International Conference on Information Security & Privacy (ICISP2015), 11-12 December 2015, Nagpur, INDIA

Multimodal Fingerprint Spoof Detection using White Light

Aadhithya Balaji, Varun. H. S, Sikha. O. K

Amrita School of Engineering, Coimbatore 641112, India

Abstract

Advancement in technology has increased the need to provide adequate security. Hence came the first security system using passwords, these systems have evolved and started using biometrics traits instead of passwords. But people have found ways to cheat such systems through different means. There have been many methods to prevent this security vulnerability, but these methods are very complex or not easy to implement. The most commonly used biometric trait for verification and also the most spoofed biometric trait is fingerprint. The need is to find an easy way to detect a fake fingerprint. The proposed system uses fingerprint and the photo of the fingernail when light is passed through is taken. The image of the fingernail is processed and features are extracted using SIFT and compared with feature vector stored in the database. The correlation is then calculated. Based on the correlation the system decides whether the fingerprint is fake or not. The system was found to react positively to intensity changes in the fingernail image and difference in the pattern of the fingernail. This system provides a simple and robust method for detection of fingerprint spoofing.

Peer-review under responsibility of organizing committee of the ICISP2015

Keywords: biometrics; multimodal; fingerprint; spoofing; fingernail; white light;

1. Introduction

"You can't change your fingerprints. You have only ten of them. And you leave them on everything you touch; they are definitely not a secret." Al Franken has captured the necessity of biometrics in this quote. Unfortunately, this old quote has been proved right in not just one but in many occasions in many interesting ways also. The world of Biometrics has evolved for more than 45 years and is still evolving. Nowadays Biometric systems have become a necessity in many places which require high security like Banks, Workplaces, Identity Cards, etc.[2]. The key to a

Peer-review under responsibility of organizing committee of the ICISP2015
doi:10.1016/j.procs.2016.02.066

successful Biometric system depends upon many aspects like how easily biometric data can be collected for testing it, how vulnerable they are to degradation due to age and impairment, how easily it can be outwitted by spoof data, etc.[1].

Biometric features are basically the physical characteristics of an individual which are distinguishable and quantifiable characteristics which can be used to identify a single person. Biometrics does not just mean fingerprints. It also includes palm veins[6], face recognition, DNA, retina scanning, iris recognition[10], fingernail matching, etc. Traditional security measures like ID card, key distribution system, passwords, etc. can easily be lost, stolen or forgotten[3]. But Biometrics has the upper hand in these cases because a fingerprint of a person can neither be lost, forgotten nor stolen (usually). Spoofing a biometric trait is fundamentally mimicking the biometric trait used to unlock the data locked by another person. Nowadays, the number of ways in which a fingerprint or any other trait can be spoofed are increasing rapidly[9] and with the progress happening in the world of technology like the evolution of 3D printers, it is becoming more and more difficult to differentiate between the real and the spoof.

Traditional Biometric systems have been using Unimodal Biometric systems for many years due to the increasing demand of accurate and efficient identification. However recent studies have proven that using a single source undergoes several problems like large-class variations, non-universality, etc., and they are more vulnerable to spoofing attacks[4]. These drawbacks can be overcome by another form of Biometrics: Multimodal Biometrics, it is the usage of two or more traits or in technical terms 'modalities' instead of using just one for the protection of your data. They use multiple sources of information to establish the identity of a person. Multimodal Biometrics based identification provides better results and gives higher accuracy compared to Unimodal Biometrics[5]. Usage of Multimodal Biometrics makes spoofing harder because it makes an imposter spoof multiple traits of a person simultaneously.

Fingerprint spoofing is the process by which individuals trick a biometric system with a fake sample. A fingerprint scanner can be spoofed by using materials which closely resemble the finger itself, for example: silicone, modeling clay, etc. The fingerprint impression is made on the material and that impression of the fingerprint is used in the scanner. A solution to detecting spoofs can be done using liveness detection and many techniques are available to check liveness like using a local descriptor[11], or using binary patterns with filters[12], etc.

In this paper, the concept of quantity light passing through the finger upon illumination with bright light is used as one of the factors for detection of fingerprint spoofing. Since each and every finger is unique with its difference in thickness and width, they play an important role in determining the transparency of the finger. This plays a major role in determining how much light will pass through the finger. This shows if the finger used in the fingerprint scanner is fake or genuine since it not only detects the amount redness (after illuminating bright light on it) of the finger which says that the finger is genuine and it will detect spoofs by comparing the original and the presently scanned one. If the finger is a fake, the difference in thickness and width of the finger and the material used to make that finger will fail in our system.

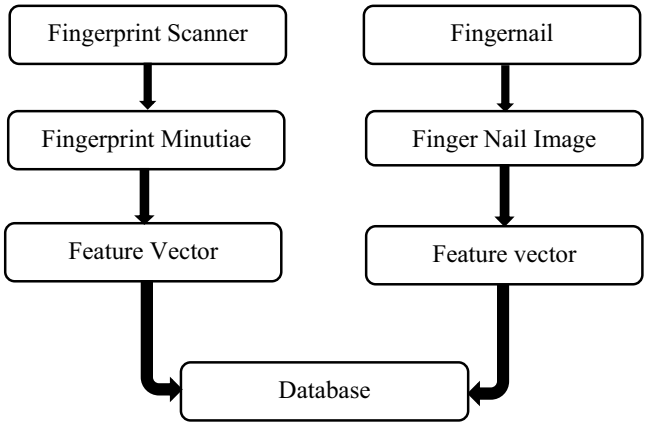

Fig. 1. Basic Architecture of the system [Enrollment].

This paper is divided into three sections. The first section explains the proposed system, the architecture and the mechanics involved in the process. Section II explains the results after experimentation. The final section gives the conclusion and the future work which could be carried out for increasing the efficiency of this proposed algorithm.

2. Proposed System

The basic architecture of the entire system is described in Fig. 1. Fingerprints are taken with the help of a finger print scanner. Minutiae points are extracted from the scanned fingerprint image and are stored in the database. Simultaneously, the picture of the finger nail is taken for processing. The finger nail region is segmented out from the input image and the features are extracted from it using SIFT. The feature vectors of both the fingerprint and finger nail is stored in the database.

During the recognition stage, image of the finger nail and fingerprint is taken and the feature vectors are made, which is then compared with the stored reference feature vector, and the correlation percentage is found. The steps involved in getting the feature vector for the finger/fingernail are:

2.1. Finger Capture

The basic design of the system is to capture the finger when it is illuminated with a bright source of light. Two powerful LEDs are used, which are placed at close distance such that the combined effect will illuminate the entire finger and a photo capturing device like a camera to capture the finger for comparison.

The light from the LEDs are distributed uniformly throughout the finger for maximizing the visibility of the finger for the camera. Non-uniform intensity distribution results in bad comparison results for recognition. The finger is placed in the designed system and is taken photo of. Fig. 2(a) and Fig. 2(c) gives two such examples of fingers taken in our system.

2.2. Preprocessing Stage

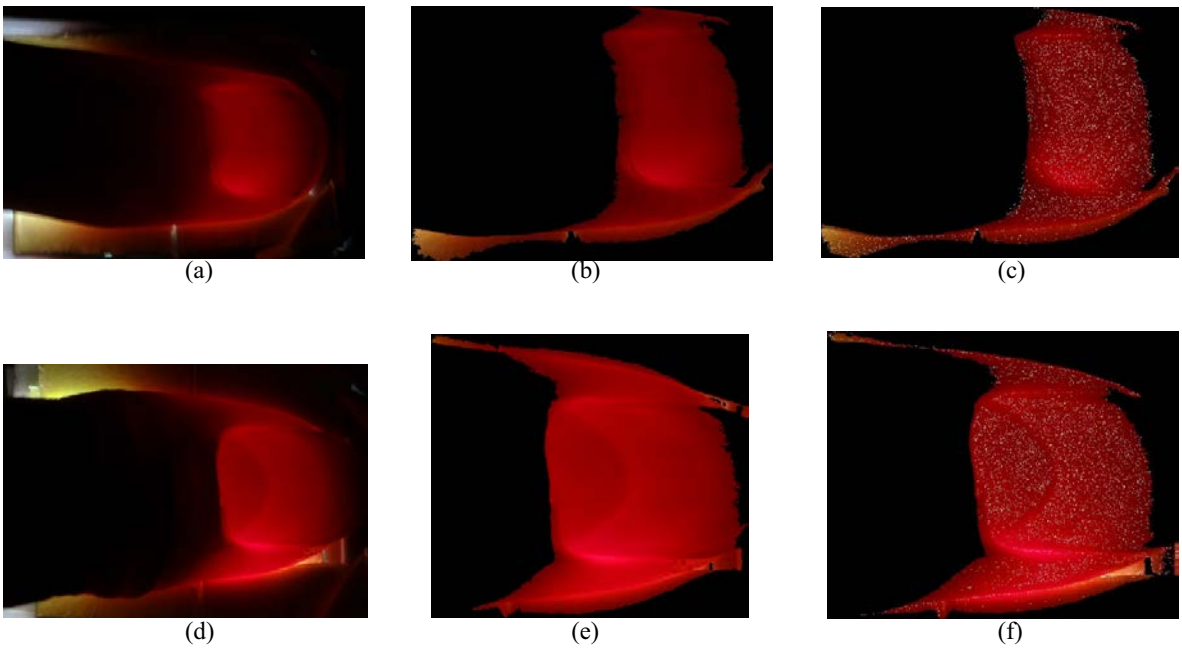

Fig. 2. (a) Input Sample 1; (b) Segmented Image of Sample 1; (c) Features Mapped on the Segmented image of Sample 1; (d) Input Sample 2; (e) Segmented Image of Sample 2; (f) Features Mapped on the segmented image of Sample 2.

In the preprocessing stage, the fingernail is extracted from the image and the regions of interest are singled out from the image. The regions of interest from the main figure are those whose intensity values lie within the desired range. This ensures that only the finger and/or the fingernail only go through the extraction process and nothing else. Segmentation of the image is done with respect to hues. The image is first separated into its respective 3 hue images. The image with the center point of the fingernail is then singled out from the set of 3 images. The image is then cropped to get only the segmented finger. The Fig. 2(b) and Fig. 2(e) gives the segmented image of the input samples.

2.3. Feature Extraction

To the regions of interest, the feature extraction is done to identify the points of interest. Feature extraction is done using Scale-invariant feature transform (SIFT) algorithm. The extracted feature key points are saved in a vector which are later used in the comparison.

A staged filtering approach is used by the SIFT algorithm which identifies stable points in the scale space[7,8]. The steps involved in the feature extraction using SIFT are:

- Scale-Space Extrema Detection: This is done by the octave generation of the Gaussian pyramid i.e. one pixel in an image is compared with its 8 neighbours as well as the 9 pixels in its previous and the next scale. If it is a local extremum, then it is a potential key point.
- Key point localization: After the potential point have been found, the have to eliminate a few of them to get accurate results. For this, Taylor series expansion is used to get a more precise location of the extrema. If this intensity value is lesser than a given threshold, it is rejected.
- Orientation Alignment: An orientation is assigned to each key point such that it is invariant to image rotation.
- Key point Descriptor: A key descriptor is created by taking the immediate neighborhood of the key point and dividing it into further sub-blocks. To each sub-block, a bin orientation histogram is created and is represented in the form of a vector.

2.4. Authentication/Recognition

During the recognition stage the fingerprint and fingernail images are obtained from the user. First a match for the fingerprint is searched for in the database using the Minutiae feature matching[13,14]. If the two fingerprints match, the features are extracted from finger nail image which is then compared with the feature vector stored in the database. For comparison of the two feature vectors, correlation is used. It computes the correlation *'r'* between two feature vectors of both the images. The match between the feature vectors is got as a value in the range of '0' to '1' depending upon how similar or exact both the images look i.e. '1' for same images and '0' for completely different images with no relation whatsoever. The matching percent is calculated from it and is checked if it crosses the threshold.

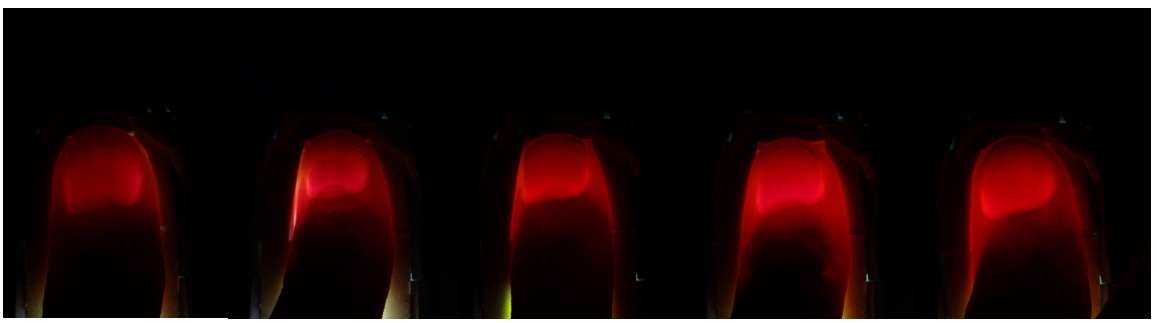

Fig. 3. Sample Images from the dataset.

2.5. Dataset

The dataset for the experimentation of the above mentioned method consisted of fingerprints and the pictures of the fingernail which are taken as a pair for each individual. Fingerprints and the fingernail pictures of around 100 people were taken. A few images from the dataset are shown in Fig.3. For experimentation, fake fingerprints were made using clay and adhesive and paired up with fingernail from our database and tested.

3. Results and Discussion

The matching percentage is calculated from the correlation coefficient. After extensive experimentation using different combinations of a fake fingerprints and the original fingernails; for the same original finger, a matching percentage of greater than 80 is got and for two completely different fingers or the original finger and its spoof, a matching percentage of less than 40 is obtained. These results are obtained by combining the fingerprint matching using the Minutiae points method for the identification of the fingerprint and this method mentioned above.

3.1. Matching Results

Here in this section, 3 cases have been taken to show the effectiveness of the algorithm. In the 1st case, the same image pair of the fingerprint and fingernail is used for both inputs. In the 2nd case, the second input is the same image pair but with a slight change in position and angle at which it was placed compared to the first image. For the

Table 1. Comparison of matching percentages

Case	Input 1	Input 2	Matching Percent (%)
1.	Finger 1	Finger 1 (Same image pair)	100
2.	Finger 1	Finger 1 (In different orientation)	> 80
3.	Finger 1	Finger 2 (Finger from different person)	< 40

3rd case, both the inputs are from completely different people. The steps mentioned in the Proposed System are carried out for the different cases and the matching percentages are calculated and compared in *Table 1*.

3.2. Vulnerabilities and Disadvantages

The combination of both fingernail and fingerprint is difficult to spoof simultaneously. This is the aspect which, is being exploited in this system. One of the most frequent method of spoofing fingerprints is by taking a mold of the original user's fingerprint. Some of the materials used in replicating the fingerprint in this method are clay, silicone and other easily moldable materials. The common thing about all these materials are that they are not fully transparent and hence impact the intensity of light visible through the fingernail and will also affect the output of the feature extraction using SIFT algorithm. The system might fail if the person whose identity is being tested wears any sort of fingernail decorations. The system also depends on the hardware being used that is if the illumination device being used has reduced brightness, the system might give incorrect results. Therefore, one of the constraints of this system depends on the brightness of the light used for capturing the image of the finger. The system detects the pattern in fingernail, and due to growth of the fingernail, the fingernail pattern might change hence the system might not give accurate results. This can be prevented by updating the database periodically. In a few cases during experimentation, the segmentation stage gave unwanted portions of the finger. This can be avoided by altering the dimensions and position of the light source and the finger. The proposed system can be implemented in the form of small device with a size comparable to that of the present fingerprint scanners.

4. Conclusion and Future Work

In this paper we have focused on how to detect and prevent spoofing with just a simple setup like illuminating the finger with white light. Although it provides a simple method, it can be improved by having a better setup to capture the finger. The segmentation algorithm can be improved such that only the fingernail and the close proximity goes through to the feature extraction stage. The SIFT algorithm used currently can be parallelized for better efficiency and speed for detection of fingerprint spoofing.

Acknowledgements

We would like to thank Mrs. Sikha. O. K and Mrs. Lalitha Mani for giving us the opportunity to work on this topic and publish a paper in the field of Biometrics.

References

1. Matthew. P, and Anderson. M, “Novel Categorisation Techniques for Liveness Detection,” Next Generation Mobile Apps, Serives and Technologies, 2014 Eighth International Conference on, Oxford, pp. 153-158, September 2014.
2. Sepasian, Mojtaba, Cristinel Mares, and Wamadeva Balachandran. "Liveness and spoofing in fingerprint identification: issues and challenges." School Of Engineering & Design Brunel University, Uxbridge, Moddlesex, Ub8 3 2010.
3. Barbosa, Igor Barros, T. Theoharis, Christian Schellewald, and Cham Athwal. "Transient biometrics using finger nails." Biometrics: Theory, Applications and Systems (BTAS), 2013 IEEE Sixth International Conference on, pp. 1-6. IEEE, 2013.
4. Peng, Jialiang, Ahmed A. Abd El-Latif, Qiong Li, and Xiamu Niu. "Multimodal biometric authentication based on score level fusion of finger biometrics." Optik-International Journal for Light and Electron Optics 125, no. 23 (2014): 6891-6897.
5. Mhaske, V. D., and A. J. Patankar. "Multimodal biometrics by integrating fingerprint and palmprint for security." In Computational Intelligence and Computing Research (ICCIC), 2013 IEEE International Conference on, pp. 1-5. IEEE, 2013.
6. Raghavendra, R., Jayachander Surbiryala, Kiran B. Raja, and Christoph Busch. "Novel finger vascular pattern imaging device for robust biometric verification." Imaging Systems and Techniques (IST), 2014 IEEE International Conference on, pp. 148-152. IEEE, 2014.
7. Lowe, David G. "Distinctive image features from scale-invariant keypoints." *International journal of computer vision* 60, no. 2 (2004): 91-110.
8. Lowe, David G. "Object recognition from local scale-invariant features." In *Computer vision, 1999. The proceedings of the seventh IEEE international conference on*, vol. 2, pp. 1150-1157. IEEE, 1999.
9. Marasco, Emanuela, and Arun Ross. "A survey on antispoofing schemes for fingerprint recognition systems." *ACM Computing Surveys (CSUR)* 47, no. 2 (2014): 28.
10. Menotti, David, Giovani Chiachia, Allan Pinto, William Robson Schwartz, Helio Pedrini, Alexandre Xavier Falcao, and Anderson Rocha. "Deep Representations for Iris, Face, and Fingerprint Spoofing Detection." *Information Forensics and Security, IEEE Transactions on* 10, no. 4 (2015): 864-879.
11. Krishna, K., and M. Narasimha Murty. "Genetic K-means algorithm." *Systems, Man, and Cybernetics, Part B: Cybernetics, IEEE Transactions on* 29, no. 3 (1999): 433-439.
12. Jia, Xiaofei, Xin Yang, Kai Cao, Yali Zang, Ning Zhang, Ruwei Dai, Xinzhong Zhu, and Jie Tian. "Multi-scale local binary pattern with filters for spoof fingerprint detection." *Information Sciences* 268 (2014): 91-102.
13. Zaeri, Naser. *Minutiae-based fingerprint extraction and recognition*. INTECH Open Access Publisher, 2011.
14. Parra, Philippe. "Fingerprint minutiae extraction and matching for identification procedure." *University of California, San Diego La Jolla, CA*: 92093-0443.